



Federal Cyber Security Research Program





Federal Cyber Security Research Program

Dr. Tomas Vagoun

Technical Coordinator, Cybersecurity R&D
National Coordination Office
Networking and IT R&D Program

William Newhouse

Scientific Advisor, Cybersecurity R&D
National Institute of Standards and
Technology (NIST)

Dr. Samuel Weber

Program Director
National Science Foundation (NSF)

Presented by Federal NITRD Program



November 20, 2010

IEEE International
Conference on
Technologies for
Homeland Security



NITRD Program

♦ Purpose

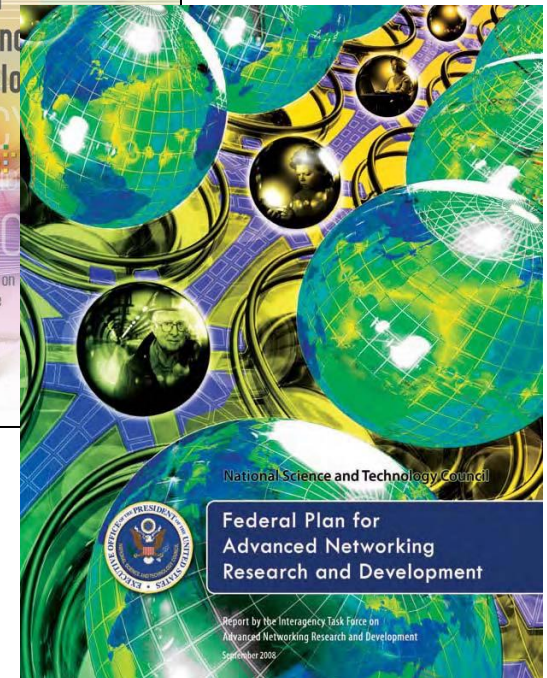
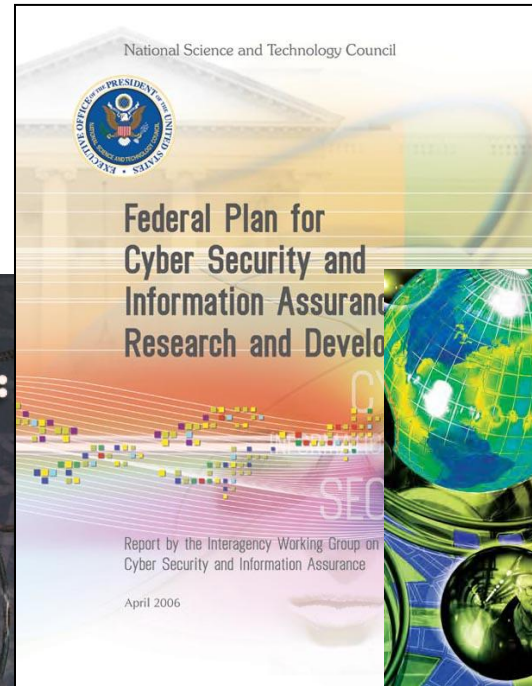
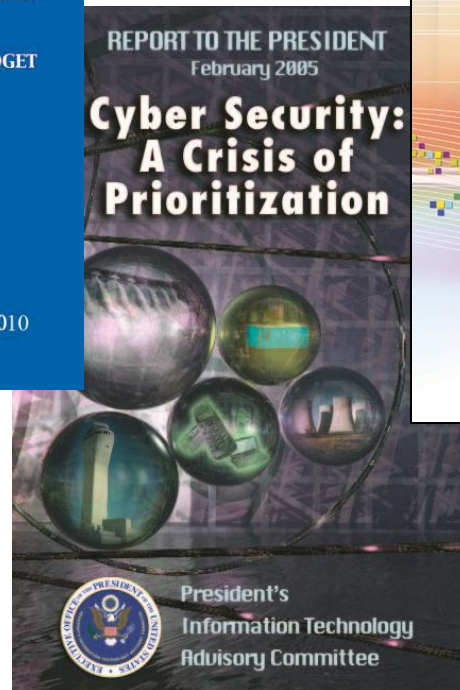
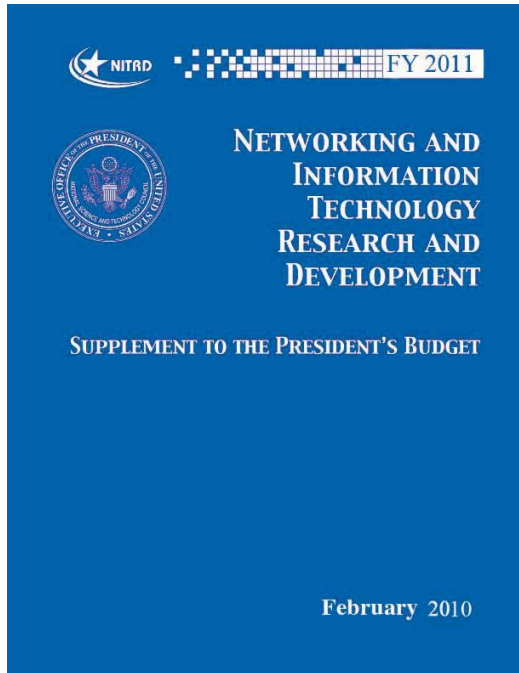
- The primary mechanism by which the U.S. Government coordinates its unclassified Networking and IT R&D investments
- Serve as a source of timely, high-quality information on critical challenges for the Federal NIT R&D
- Support NIT-related policy making in the White House Office of Science and Technology Policy (OSTP)
- Established by the High-Performance Computing Act of 1991

♦ Scope

- Approximately \$4B/year across 14 agencies, seven program areas
- Cyber Security and Information Assurance (CSIA)
- Human Computer Interaction and Information Management (HCI&IM)
- High Confidence Software and Systems (HCSS)
- High End Computing (HEC)
- Large Scale Networking (LSN)
- Software Design and Productivity (SDP)
- Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW)



NITRD Publications





Selected Agency R&D Budgets in Cyber Security and Information Assurance

Selected NITRD Agencies	Cyber Security and Information Assurance R&D (Unclassified) FY 2010 Budget Estimates
DARPA	\$143M
DOD (OSD, ARL, AFRL, ONR)	\$94M
NSF	\$71M
DHS S&T	\$37M
NIST	\$37M
NSA	\$29M

Source: "NITRD Supplement to the President's FY 2011 Budget,"
<http://www.nitrd.gov/pubs/2011supplement/FY11NITRDSupp-FINAL-Web.pdf>



Federal Coordinated Effort on Game-Changers

- ♦ Strong commitment to focus on **game-changing** technologies for **coordinated** cybersecurity R&D agenda
 - Comprehensive National Cybersecurity Initiative
 - Cyberspace Policy Review
 - White House S&T Priorities for FY12 Budget
 - Howard Schmidt, White House Cybersecurity Coordinator
 - Aneesh Chopra, President's Chief Technology Officer
- ♦ It's about **trustworthiness** of digital infrastructure
 - Security, reliability, resiliency, privacy, usability
 - How can we:
 - Enable risk-aware safe operations in compromised environments
 - Increase adversaries' costs and exposure
 - Support informed trust decisions



Three-pronged Approach

- ◆ Themes
- ◆ Science of Cyber Security
- ◆ Transition to Practice



Attributes of a Good Research Theme

- ◆ Compels a new way of operating or doing business
- ◆ Draws on a number of sciences and technologies (is not a single technology area)
- ◆ Is interdisciplinary
- ◆ Pokes at least one hard problem
- ◆ Requires a multi-year effort with measurable achievements
- ◆ Presents a path to transition, deployment, and to cooperation with the private sector
- ◆ Encourages research be conducted with an adversarial perspective



Initial Themes

- ◆ Tailored trustworthy spaces
 - Supporting context specific trust decisions
 - Basing trust decisions on verified assertions
- ◆ Moving target
 - Providing resilience through agility
 - Attacks only work once if at all
- ◆ Cyber economics and incentives
 - Providing incentives to good security
 - Providing disincentives to cyber crime

Remember: These are just starting points



Some Potential New Themes

- ◆ Design for Assurance (security engineering, practical verification, system architecture, usability)
- ◆ Understanding the Cyber Environment (situational awareness, systemic understanding of vulnerability)
- ◆ Nature-inspired Solutions (self-healing, evolving, growth)
- ◆ Mobility
- ◆ Borderless Security



New Emphasis Area: Science of Cyber Security

- ◆ A major research initiative on the *science of cyber security* that
 - Is aggressive in nature
 - Supports interdisciplinary efforts
 - Supports high-risk explorations to establish such a scientific basis
 - Is integrated in a cohesive whole to produce results that impact large-scale systems
 - Advances the ultimate goal of protecting deployed systems
 - Is grounded in public-private partnership of government agencies, universities, and industry



Scientific Methods

- ♦ Not limited to traditional formal, mathematical model of science
 - This is an important aspect, but perhaps not the most important
- ♦ Includes experimental science, field studies, social and behavioral science, principles of engineering
 - Considerations of shared data set, test methods and facilities
- ♦ Aimed at providing repeatability, robust scientific discourse, grounding for research decisions, ability to guide new research efforts

Some Key Science of Cyber Security Research Thrusts

- ◆ Methods to model adversaries
- ◆ Techniques for component, policy and system composition
- ◆ A control theory for maintaining security in the presence of partially successful attacks
- ◆ Sound methods for integrating the human in the system: usability and security
- ◆ Quantifiable, forward-looking, security metrics (using formal and stochastic modeling methods)
- ◆ Measurement methodologies and testbeds for security properties
- ◆ Development of comprehensive, open, and anonymized data repositories



Transition to Practice

- ◆ Concerted effort to get results of federally funded research into broad use
 - Integrated demos
 - Conferences and workshops
 - “Matchmaking” efforts
 - Among Agencies
 - Between research and product
 - Potential funding for last mile



Initial Cybersecurity R&D Themes

William Newhouse

Scientific Advisor, Cybersecurity R&D

National Institute of Standards and Technology



Why The Themes

- ◆ Theme \neq Hard Problem
- ◆ To compel a new way of operating / doing business
- ◆ To attack underlying causes to bring about changes
- ◆ Themes draw on a number of sciences and technologies (are not a single technology area)
- ◆ Themes present a path to transition, deployment, and cooperation with the private sector



Tailored Trustworthy Spaces

In the physical world, we operate in many spaces with many characteristics

- Home, school, workplace, shopping mall, doctor's office, bank, theatre
- Different behaviors and controls are appropriate in different spaces

Yet we tend to treat the cyber world as a homogenous, undifferentiated space

The vision is of a flexible, distributed trust environment that can support functional, policy, and trustworthiness requirements arising from a wide spectrum of activities in the face of an evolving range of threats

TTS Paradigm

- ◆ Users can select/create different environments for different activities satisfying variety of operating capabilities
 - Confidentiality, anonymity, data and system integrity, provenance, availability, performance
- ◆ Users can negotiate with others to create new environments with mutually agreed characteristics and lifetimes

TTS Challenges

- ◆ Specifying a tailored trustworthy space
- ◆ Policy specification and management
- ◆ Validation of platform integrity
- ◆ Violation detection
- ◆ Verifiable separation

Moving Target

- ◆ Controlled change across multiple system dimensions to:
 - Increase uncertainty and apparent complexity for attackers, reduce their windows of opportunity, and increase their costs in time and effort
 - Increase resiliency and fault tolerance within a system



MT Paradigm

- ♦ All systems are compromised; perfect security is unattainable
- ♦ Objective is to continue safe operation in a compromised environment, to have systems that are defensible, rather than perfectly secure

MT Research Challenges

- ♦ Abstractions and methods for scientific reasoning about MT mechanisms and their effectiveness
- ♦ Understanding system characteristics and the degrees of their movement, in terms of both entropy and movement intervals, where MT mechanisms are most effective
- ♦ Management methods for MT systems
- ♦ Methods for cost-benefit analysis of MT techniques
- ♦ Adaptability and evolution of MT mechanisms to increase their effectiveness
- ♦ Ecosystem of programming languages, tools, architectures, and testing capabilities for MT systems
- ♦ Integration with legacy systems



Cyber Economics & Incentives

- ◆ A focus on what impacts cyber economics and what incentives can be provided to enable ubiquitous security:
 - New theories and models of investments, markets, and the social dimensions of cyber economics
 - Data, data, and more data with measurement and analysis based on that data
 - Improved SW development models and support for “personal data ownership”



CEI Paradigm

- ◆ Data for everyone, anytime, anywhere
- ◆ Security deployment decisions based on knowledge, metrics, and proper motivations
- ◆ Properly incentivized vendors
- ◆ Individual users taking ownership of their personal data
- ◆ Critical infrastructure providers able to better defend their networks and systems



CEI Challenges

- ◆ Data
 - Legal and ethical collection and distribution
 - Lack of appropriate data to support effective economic analysis
- ◆ Empowerment of critical infrastructure providers
 - Provide legal frameworks allowing service providers to be more active in defense of their systems/services
- ◆ Personal Info/Behavior
 - Educating/incentivizing users about the benefits of secure practices and acceptable cyber behavior
 - “Personal Data”



Initiating Cybersecurity R&D Themes: Current Activities

Dr. Samuel Weber

Program Director
National Science Foundation





Selected Current Activities

- ◆ NSF's Workshop on the Future of Trustworthy Computing
- ◆ DARPA's CRASH program
- ◆ IARPA's STONESOUP
- ◆ Workshop on Cyber Security Data for Experimentation
- ◆ DHS's Cyber Security Industry Day



NSF Workshop on the Future of Trustworthy Computing

- ◆ Goals:
 - Introduce and stimulate ideas about NITRD cybersecurity R&D themes in research community
 - Assist newer researchers in finding productive research directions
- ◆ Occurred Oct. 27-29th
 - ~100 attendees in-person, mix of new and experienced
 - Recorded online: <http://tc2010.cse.psu.edu/index.html>
- ◆ Keynotes from
 - David Reed, *SAP Labs*
 - Virgil Gligor, *Carnegie-Mellon University, CyLab*
 - Daniel Geer, *In-Q-Tel*
 - Patrick Lincoln, *SRI International*



NSF Workshop: Panels

♦ Tailored Trustworthy Spaces

- Chair: Joshua Guttman, *Worcester Polytechnic Institute*
- William Arbaugh, *University of Maryland*
- Carl Gunter, *University of Illinois, Urbana-Champaign*
- Ruby Lee, *Princeton University*

♦ Moving Targets

- Chair: Sal Stolfo, *Columbia University*
- Anup Ghosh, *George Mason University*
- John Knight, *University of Virginia*
- Tal Rabin, *IBM Research*

♦ Cyber-economics

- Chair: Rebecca Wright, *Rutgers University*
- Matt Blaze, *University of Pennsylvania*
- Jens Grossklags, *Princeton University*
- Rafael Pass, *Cornell University*

♦ Science of Cybersecurity

- Chair: Mike Reiter, *University of North Carolina*
- Andrew Appel, *Princeton University*
- Amit Sahai, *University of California, Los Angeles*
- Peter Weinberger, *Google*

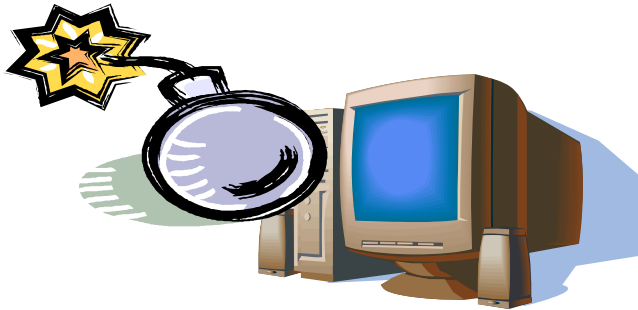


NSF Workshop: Other Events

- ◆ NITRD panel
 - Bill Newhouse, *NIST Information Technology Lab*
 - Douglas Maughan, *DHS S&T*
 - Steven E. King, *Office of the Director, Defense Research & Engineering*
 - Sandy Landsberg, *DoE*
- ◆ Breakout sessions on each theme

DARPA's CRASH Program

Clean-slate design of **Resilient, Adaptive, Secure Hosts**



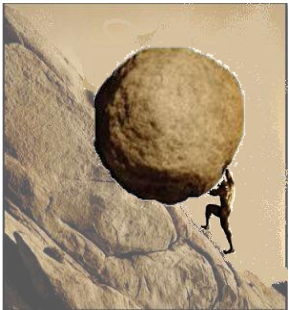
*Blow off the Legacy Computational Base
Inspired by biological mechanisms for
resilience*

- Provably removes whole classes of vulnerabilities
- Learns how to respond to new threats
- Defense in depth
- Diversity, randomization, variability
- Diagnosis, adaptation & self-regeneration

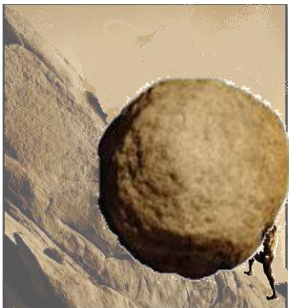
Make The Enemy Push the Rock



Innate immunity rules out all the standard attacks using hardware mechanisms that cannot be bypassed. There are at least two reasons why any attack won't work, both of which would need to be subverted for the attacker to make progress. Even if an attacker gains some access, his ability to exploit the penetration is limited by the hardware enforced access rules.



Adaptive immunity learns to recognize the footprints of novel techniques used by the attacker, catches him earlier in the exploit, prevents him from achieving his goals, and facilitates quicker recovery and regeneration. Innate immunity buys us time for adaptive immunity to take over and increase the attacker's work factor yet further. As time goes on we know more and more about the attacker and how to stop him.



Dynamic Diversity guarantees that even if an attacker gets past both innate and adaptive immunity, he still has more work to do because what he thought he knew about us is no longer true. As time goes on we know more and more about the attacker while he knows less about us.



Program Structure

Program Area	Topics
New Processor Design	Innate immunity Type & memory safety, Meta-data processing
New OS and Language System Design	Innate & Adaptive Immunity, Diversification Decomposition, separation, least privilege, complete mediation, separation of privilege, information flow management
Application middleware	Adaptive Immunity & Diversification System modeling & machine learning, self monitoring and diagnosis, self-adaptive software frameworks, automatic patching, memory and instruction set randomization
Formal methods & analysis techniques	Assessing resilience, metrics, co-design of hardware, languages, OS and formal methods, information flow proofs, verification of security properties
Application demonstrators	New demo min-apps built to exploit, demo, & test full framework
Red teaming	Red-teams help design & test from the beginning
Incentives and market analysis	Workshops and analyses of opportunities & incentives for transitioning technologies into DoD & mainstream

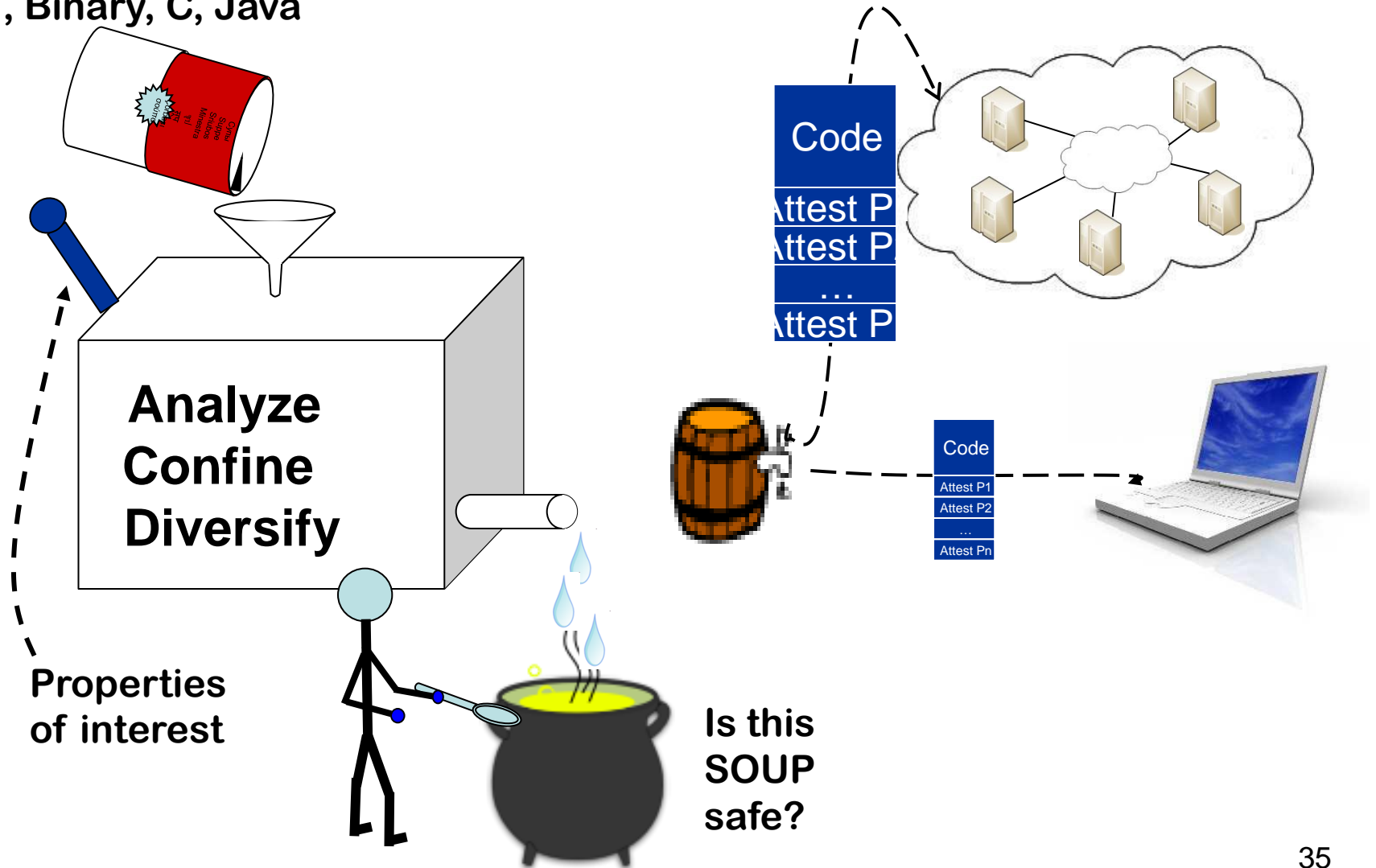


IARPA's STONESOUP

- ♦ “Securely Taking on New Executable Software of Uncertain Provenance”
- ♦ Develop technology that will allow end users to invoke:
 - advanced automated software analysis techniques to identify vulnerabilities or to assure their absence
 - *tailored confinement* of software execution so that identified weaknesses cannot be exploited
 - *diversification* of software components so residual vulnerabilities will be more difficult for attackers to discover or exploit
- ♦ High-risk, high-reward: putting tools in the hand of end-users
 - Opportunity to provide feedback to software vendors

STONESOUP Vision

e.g., Binary, C, Java





Workshop on Cyber Security Data for Experimentation

- ◆ Goal: Bring together academics, companies and government agencies to discuss
 - models of engagement to allow the research community to conduct experiments with real-world data sets
 - how to share research results
 - how funding agencies can facilitate the process
- ◆ Sponsored by NSF, DHS, ONR, Treasury, and others
- ◆ http://www.gtisc.gatech.edu/nsf_workshop10.html
- ◆ Industry involvement
 - Symantec, McAfee, Verisign, Microsoft, Cisco
- ◆ NSF plans to support industry/academic data sharing as result of workshop



DHS Cyber Security Industry Day

- ◆ Industry Day Session

- Nov. 17, in Washington DC
- https://www.fbo.gov/spg/DHS/OCPO/DHS-OCPO/Cyber_Security_Industry_Day/listing.html
- DHS S&T Cybersecurity R&D BAA will be upcoming

- ◆ Goals:

- Provide the tools necessary to increase resilience to cyber threats and operational disruptions and the forensic tools to identify perpetrators
- Engage industry, government, and academia to ensure that the core functions of the internet develop securely and benefit all owners, operators, and users
- Address economic assessment, risk analysis, and modeling requirements to implement and deploy cyber security technologies
- Accelerate transition of new cyber security technologies into products and services for end users including DHS, first responders, critical infrastructure providers and sectors, private industry, and government



Other Agency Activities

♦ DoD

- ARO: Workshop on Moving Target Defense, GMU, Oct. 25-26
- AFOSR: Fall 2010 MURI topic on Science of (Cyber) Security

♦ NIST

- Active areas include: virtualization and cloud, key management, usability of security, identity management, health IT, Smart grid
- Recent activity: Second Cloud Computing Forum & Workshop Nov. 4-5 2010; see: <http://www.nist.gov/itl/cloud/cloudworkshopii.cfm>

♦ Treasury

- Sept. 2010 workshop on Financial Services Explained: An Operational Overview

♦ DoEnergy

- \$30M in cyber security project awards announced Sept. 23, 2010: <http://www.energy.gov/news/documents/Cybersecurity-Selections.pdf>
- Office of Electricity Delivery and Energy Reliability: joint funding with DHS of Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) , spring 2010
- Office of Science: basic research in mathematics of cybersecurity and complex interconnected systems underway

Conclusions

- ◆ Coordinated effort among government agencies
- ◆ Focus on game-changing themes
 - Encourages research collaborations based on tangible topics
 - Common vocabulary to relate different research activities
 - Will be aware of and reactive to new research directions
- ◆ Open to new collaborations, especially between government, industry and academia



For More Information

Tomas Vagoun, PhD
CSIA IWG Technical Coordinator

National Coordination Office for
Networking and Information Technology Research and Development
Suite II-405, 4201 Wilson Blvd.
Arlington, VA 22230
Tel: (703) 292-4873
vagoun@nitrd.gov

<http://www.nitrd.gov>

<http://cybersecurity.nitrd.gov>